

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-6, 8-16, and 18-22 are currently pending, Claims 1-6, 8-16, and 18-22 having been amended, and Claims 7 and 17 having been canceled. The changes and additions to the claims do not add new matter and are supported by the originally filed specification, for example, in original Claims 7 and 17.

In the outstanding Office Action, Claims 21-22 were rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter; Claims 1-2, 11-12, and 21 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite; Claims 1, 3-5, 8, 11, 13-15, 18, and 21 were rejected under 35 U.S.C. §102(b) as anticipated by Kuo et al. (*Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm*, hereafter “Kuo”); and Claims 2, 7, 9, 10, 12, 17, 19-20, and 22 were rejected under 35 U.S.C. §103(a) as unpatentable over Kuo in view of Lin et al. (GB 2345229A, hereafter “Lin”).

With respect to the rejection of Claims 21-22 under 35 U.S.C. §101, Applicants respectfully submit that amending Claims 21 and 22 to recite a statutory computer-readable storage medium overcomes this ground of rejection.

With respect to the rejection of Claims 1, 11, and 21 under 35 U.S.C. §112, second paragraph, Applicants respectfully submit that the amendment to Claims 1, 11, and 21 removes the antecedent basis issue and therefore this ground of rejection has been overcome.

With respect to the rejection of Claims 2 and 12 under 35 U.S.C. §112, second paragraph, the Office Action takes the position that the phrase “dummy encryption process” is not clear within the claim. However, Applicants respectfully submit that the phrase “dummy encryption process” is described in amended Claims 1 and 11 as a “process that is

unnecessary for said original encryption processing sequence in at least one of said groups of divisions.” (See also original Claims 2 and 12, and page 5, line 21 to page 6, line 1 of the specification). Therefore, Applicants respectfully submit that this rejection has been overcome.

With respect to the rejection of Claim 1 under 35 U.S.C. §102(b), Applicants respectfully submit that the amendment to Claim 1 overcomes this ground of rejection.

Amended Claim 1 recites, *inter alia*,

wherein the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process, and

said control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups of divisions, and sets the number of dummy single-DES processes to be set to a multiple of 3 corresponding to the triple-DES encryption process.

Applicants respectfully submit that Kuo and Lin fail to disclose or suggest these features of Claim 1.

Kuo describes a method of optimizing a ASIC processor that implements the AES Rijndael encryption algorithm. The Rijndael algorithm is a replacement algorithm for the DES and Triple DES algorithm (see page 1, Introduction section). In Kuo, a device implementing the Rijndael algorithm receives a 256 bit data word that is to be encrypted. The encryption process is broken down into 4 sub-modules (see Section 3.5.1). In the first sub-module the 256 bit data word is divided into 32 8-bit chunks. An S-box look-up table is applied to each 8-bit chunk simultaneously so that each 8-bit chunk is translated into a different 8-bit chunk based on the output of the look-up table, and then the output data is merged into a new 256 bit data word. In the second sub-module, the new 256 bit data word is divided again and then the bits are shifted. In the third sub-module, the 256 bit data word

output from the second sub-module is mixed by a multiplication algorithm. In the fourth-sub-module, the mixed 256 bit data is then XORed with 256 bit keys to generate a final result.

The Office Action takes the position that Kuo discloses a method using a single-DES and triple-DES process because Kuo describes an S-box look-up table in the first encryption sub-module and single DES also uses an S-box lookup table (see Office Action at page 6 and page 7, citing page 56, section 3.5.1 of Kuo). However, if two algorithms use an S-box look-up table as a sub-part of a longer process, it does not make them the same algorithm. As discussed above, the AES Rijndael algorithm includes a 4 sub-module process that is different from DES. In fact, Kuo describes that the AES Rijndael algorithm is an expected replacement to the DES and triple-DES encryption process (see page 1 of Kuo). A device incorporating the AES Rijndael encryption algorithm, as described in Kuo, is encrypting information differently than a device incorporating a single-DES or triple-DES algorithm. Thus, Kuo, which describes the AES Rijndael encryption algorithm, is not relevant to the invention defined by Claim 1.

Therefore, Kuo fails to disclose or suggest an encryption processing apparatus where the original encryption processing sequence to be mixed is an encryption processing sequence including a triple-DES encryption process, and the control section is configured to set a dummy single-DES process as a dummy encryption process that is unnecessary for the original encryption processing sequence in at least one of said groups of divisions, and sets the number of dummy single-DES processes to be set to a multiple of 3 corresponding to the triple-DES encryption process, as defined by Claim 1.

Lin has been considered but fails to remedy the deficiencies of Kuo in regards to amended Claim 1. Lin describes an encryption system to protect against differential power analysis attacks for a DES system. However, as discussed above, Kuo is directed to the AES

Rijndael encryption algorithm, and not DES. Accordingly, there is no suggestion in Kuo or Lin to replace the primary encryption algorithm used in Kuo with the DES algorithm used in Lin.

Additionally, the Office Action takes the position that Lin describes setting a dummy-single-DES process as a dummy encryption process and setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple-DES (see Office Action at page 11, citing page 11, lines 10-28 of Lin). However, Lin describes inserting dummy S-block lookups into a real DES process (see page 11, lines 10-13), but Lin does not describe making an entire single-DES process as a dummy itself. Inserting dummy S-block lookups into an actual DES process to be used, is not the same as inserting an entire dummy single-DES process. In other words, in Lin, the “dummy” that is being inserted is an S-block lookup within a real DES process (see page 11, lines 23-25, stating, “[p]referably one performs at least on dummy look-up (and more preferably 2-4 dummy look-ups) for each real look-up”). However, the invention defined by Claim 1 is directed to setting a whole single-DES process as a dummy (see Figure 7B and page 30, lines 19-24) and not just S-block lookups (see specification, at Figure 7B and page 30, lines 19-24).

Additionally, Lin fails to disclose or suggest using a triple-DES encryption process. When using a triple-DES process, it is advantageous to insert dummy single DES processes at multiples of 3 so that each process is difficult to distinguish from a non-dummy triple-DES process when viewed from an external analyzer (see specification, at page 29, line 10 to page 30, line 4). However, Lin only describes an encryption system to protect against differential power analysis within a single DES process (see page 5, lines 23-32 and page 11, lines 10-13)

Therefore, Lin fails to disclose or suggest setting a dummy single-DES process as a dummy encryption process unnecessary for the original encryption processing sequence in at

least one of said groups of divisions, and setting the number of dummy single-DES processes to be a multiple of 3 corresponding to the triple DES encryption process, as defined by amended Claim 1.

Moreover, as Kuo describes the AES Rijndael algorithm, and Lin describes single DES, none of the references suggest using triple DES as done in Claim 1.

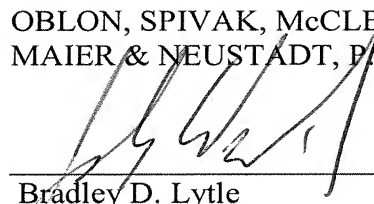
Thus, it is respectfully submitted that amended Claim 1 (and all associated dependent claims) patentably distinguishes over Kuo and Lin, either alone or in proper combination.

Amended independent Claims 9, 11, 19, 21, and 22 recite features similar to those of amended Claim 1 discussed above. Therefore, it is respectfully submitted that amended Claims 9, 11, 19, 21, and 22 (and all associated dependent claims) patentably distinguish over Kuo and Lin, either alone or in proper combination.

Consequently, in light of the above discussion and in view of the present amendment, the outstanding grounds for rejection are believed to have been overcome. The present application is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Joseph Wrkich
Registration No. 53,796